

**THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA**

Nicole Toussaint,

individually and on behalf of all others
similarly situated,

Plaintiff(s),

v.

HanesBrands, Inc.,

Defendant.

Case No.:_____

CLASS ACTION COMPLAINT

Jury Trial Demanded

PLAINTIFF(S)' CLASS ACTION COMPLAINT

Plaintiff(s) Nicole Toussaint (“Plaintiff(s)”), individually and on behalf of all others similarly situated, bring this action against Defendant HanesBrands, Inc. (“HBI” or “Defendant”) to obtain damages, restitution, and injunctive relief for the Class, as defined below. Plaintiff(s) make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant HBI (the “Data Breach”), which held in its possession certain personally identifiable information (“PII” or “the Private Information”) of Plaintiff(s) and other individuals (the “Class”) by Defendant HBI. This Data Breach (a ransomware attack) was first detected by HBI on or around May 24, 2022.

2. The Private Information compromised in the Data Breach included certain highly sensitive personal and protected health information of current and former employees, including Plaintiff(s), and other individuals. This Private Information included, but is not limited to: name, address, date of birth, financial account information, government-issued identification numbers such as driver's license, Passport and Social Security number, and other information related to benefits and employment, including sensitive health information collected for employment-related purposes.¹

3. The Private Information compromised in what HBI refers to as a “data security incident” was copied—*i.e.*, exfiltrated—by cyber-criminals who intentionally targeted HBI for the highly sensitive Private Information it collects, then perpetrated the attack. As a result, the Private Information of Plaintiff(s) and Class remains in the hands of those cyber-criminals or has been sold on the “dark web” (as HBI admits is a risk that it continues to monitor, *see* Ex. A).

4. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for employment or other business purposes.

5. Plaintiff(s) bring this class action lawsuit on behalf of themselves and all others similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide

¹ See Plaintiff's Notice Letter, attached as Exhibit A.

timely and adequate notice to Plaintiff(s) and other Class Members of exactly what of their Private Information was subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant HBI's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff(s)' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Defendant disregarded the rights of Plaintiff(s) and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff(s)' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and Class Members with prompt and full notice of the Data Breach.

8. In addition, Defendant HBI failed to properly monitor the computer network and systems that housed the Private Information. Had HBI properly monitored its property, it would have discovered the intrusion sooner.

9. Plaintiff(s)' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant HBI collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiff(s) and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff(s) and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff(s) and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Through this Complaint, Plaintiff(s) seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiff(s) seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including

improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiff(s) brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, (iv) invasion of privacy; and (v) unjust enrichment.

PARTIES

16. Plaintiff Nicole Toussaint is and at all times mentioned herein was an individual citizen of the State of Maine, residing in the city of Penobscot (Hancock County), and is a former employee of Defendant. Ms. Toussaint received notice of the Data Breach dated August 16, 2022, attached as Exhibit A.

17. Defendant HanesBrands, Inc. is a North Carolina Business Corporation company with its principal place of business at 1000 E. Hanes Mill Road, Winston-Salem, North Carolina 27105.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, there are more than 100 Class Members, and at least one Class Member, including Plaintiff(s) Nicole Toussaint, is a citizen of a state different from Defendant.

19. The Court has personal jurisdiction over Defendant because it is headquartered in this District, has its principal place of business in this District, and regularly conducts business in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiff(s)'s claims occurred in, were directed to and/or emanated from this District, Defendant is based in this District, and maintains Plaintiff(s)'s and Class Members' PII in the District.

FACTUAL ALLEGATIONS

Defendant's Business

21. Defendant HanesBrands, Inc. manufactures and sells apparel under the brand names HBI, Champion, and Bonds. HBI currently employs 59,000 associates in 33 countries.²

22. HanesBrands, Inc. is one of the world's largest producers of clothing. HanesBrands sells clothing under well-known brand names, including Hanes, Champion, Bali, Berlei, Bonds, Bras N Things, ComfortWash, Gear for Sports, JMS/Just My Size, Maidenform, Playtex, and Wonderbra.

23. For the purposes of this Class Action Complaint, all of HBI's associated locations and/or subsidiaries that were affected by this Data Breach will be referred to collectively as "HBI."

24. In the ordinary course of employment or seeking employment with Defendant HBI, each applicant and/or employee must provide (and Plaintiff(s) did provide) Defendant HBI with sensitive, personal, and private information, such as their:

² <https://www.HBI.com/corporate?section=company> (last accessed Oct. 13, 2022).

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;
- Marital status;
- Demographic information;
- Driver's license, and state or federal identification (*e.g.* Passport);
- Personal health information and disclosures required for job requirements;
- Other personal information related to and necessary to receive employment

benefits and employment; and

- Bank account numbers, financial institution, and/or credit card information.

25. Although HBI claims in its Notice Letters that “the safety of [former and current employee] personal information is of the utmost importance to [it],”³ HBI does not follow its own policies or industry standard practices in securing employee's PII.

26. In its very short and vague “Corporate Privacy Notice,” HBI tells its employees (including Plaintiff(s) and the Class) that: “We maintain reasonable administrative, technical and physical safeguards to protect your Personal Information.”⁴

27. Yet, through its failure to properly secure the Private Information of Plaintiff(s) and Class, HBI has not adhered to its own promises of protecting employees' privacy rights.

³ See Plaintiff's Notice Letter, Exhibit A

⁴ <https://www.Hanes.com/corporate?section=company> (last accessed October 12, 2022)

28. The current and former employees' (and upon information and belief, employees' dependents') information held by Defendant HBI in its computer system and network included the highly sensitive Private Information of Plaintiff(s) and Class Members.

The Data Breach

29. A ransomware attack occurs when cyber criminals intend to access a computer system for criminal purposes, then do actually access and steal Private Information (the "Data Breach") that has not been adequately secured by a business entity like HBI. Often, the business that experiences a ransomware attack is forced to pay hundreds of thousands of dollars to even access its own computers again.

30. According to the "Notice of Security Incident" that HBI mailed to current and former employees and other affected individuals, *i.e.*, Class members, "[o]n May 24, 2022, [it] detected a ransomware incident impacting certain internal IT systems." Its investigation "recently identified that some of [Class members'] personal information was impacted in the event."⁵

31. However, without further explanation, in its notice letter HBI claims that "We take the security of all information in our control very seriously."⁶ Then it claims to be "tak[ing] a number of steps to even further strengthen the security of our networks." Additionally, HBI tacitly admits that the risks of identity theft are substantial and imminent because it is "continuing to monitor the dark web for any indication of misuse of personal

⁵ See Exhibit A

⁶ *Id.*

information in connection with this incident . . .” However, HBI does not indicate how it is monitoring the dark web, and whether (or how) it will inform Class members if it discovers (or has already discovered) their stolen Private Information on the dark web.⁷

32. The Notice of Data Security Incident mailed specifically to Plaintiff Toussaint also states that the PII stolen “may have included contact information; date of birth; financial account information; government issued identification numbers such as drivers’ license numbers, passport information and social security numbers; and other information related to benefits and employment, including certain limited health information provided for employment-related purposes.”⁸

33. As reported to some State Attorneys General in its Data Breach Notifications (“breach report”) on May 24, 2022, HBI’s investigation revealed that the Private Information (including both PII some limited PHI) of an unknown number of individuals was accessed in this Data Breach.⁹

34. Plaintiff(s) and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

⁷ *Id.*

⁸ *See* Exhibit A

⁹ *See, e.g.*, <https://apps.web.maine.gov/online/aeviewer/ME/40/6f9be6c4-7e0f-4015-a7b1-1d6dcc66ccd1.shtml> (last visited October 12, 2022).

Defendant Fails to Comply with FTC Guidelines

35. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

36. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.¹⁰ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹¹

37. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

¹⁰ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited October 12, 2022).

¹¹ *Id.*

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

38. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect employee data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

39. Defendant failed to properly implement basic data security practices.

40. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to employees’ PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

41. Defendant was at all times fully aware of its obligation to protect the PII and of its applicants, past and current employees, their dependents, and other individuals from whom it collected and stored PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

42. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data

unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

43. Other best cybersecurity practices that are standard in business include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

44. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

45. These foregoing frameworks are existing and applicable industry standards in business, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant has Breached its Obligations to Plaintiff(s) and Class

46. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard HBI's computer systems and the Class members' PII stored on its networks. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect past and current employees' and other individuals' Private Information;
- c. Failing to properly and continuously monitor its own data security systems for existing intrusions;
- d. Failing to ensure that vendors with access to individuals' PII data employed reasonable security procedures;
- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- f. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

47. As the result of maintaining its computer systems in manner that required security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff(s)' and Class Members' Private Information.

48. Accordingly, as outlined below, Plaintiff(s) and Class Members now face an imminent and substantial risk of fraud and identity theft.

***Data Breaches Put Consumers at an Increased Risk
Of Fraud and Identify Theft***

49. Data Breaches such as the one experienced by HBI's employees and other individuals are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

50. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."¹²

51. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.¹³

52. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

53. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use

¹² See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited October 12, 2022) ("GAO Report").

¹³ See <https://www.identitytheft.gov/Steps> (last visited October 12, 2022).

the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

54. Theft of Private Information is also gravely serious. PII is a valuable property right.¹⁴

55. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

56. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

57. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff(s) and Class Members are at an increased risk of fraud and identity theft for many

¹⁴ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

years into the future. Thus, Plaintiff(s) and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

58. Sensitive Private Information can sell for as much as \$363 per record according to the Infosec Institute.¹⁵ PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

59. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.¹⁶ Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.¹⁷ Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

60. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may

¹⁵ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited October 12, 2022).

¹⁶ *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited October 12, 2022).

¹⁷ *Id.* at 4.

not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”¹⁸

61. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”¹⁹

62. In recent years, employers have experienced disproportionately higher numbers of data theft events than in the past. Defendant therefore knew or should have known of this heightened risk and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFF(S)’ EXPERIENCES

Plaintiff Nicole Toussaint

63. Plaintiff Nicole Toussaint is and at all times mentioned herein was an individual citizen residing in the State of Maine, in the city of Penobscot (Hancock County).

¹⁸ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited October 12, 2022).

¹⁹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited October 12, 2022).

64. Plaintiff Toussaint is and was a former employee of Defendant at all times relevant to this Complaint.

65. Plaintiff Toussaint was employed at HBI as an Assistant Manager from the years 2012 through 2018.

66. Plaintiff Toussaint received a Notice of Data Breach Letter, related to HBI's Data Breach that is dated August 16, 2022. *See* attached as Exhibit A.

67. The Notice Letter that Plaintiff received states that her stolen information "may have included contact information; date of birth; financial account information; government issued identification numbers such as drivers' license numbers, passport information and social security numbers; and other information related to benefits and employment, including certain limited health information provided for employment-related purposes." *See* Exh. A. Her Notice Letter lacks specificity about the exact information breached.

68. Plaintiff Toussaint is especially alarmed by the amount of stolen or accessed PII listed on her letter, and even more by the fact that her Social Security number was identified as among the breached data on HBI's computer system.

69. Since the Data Breach, Plaintiff Toussaint monitors her financial accounts for as much as two hours per day. Having to spend this huge amount of time every week not only wastes her time as a result of HBI's negligence, but it also causes her great anxiety. She checks her credit reports periodically for any issues.

70. Plaintiff Toussaint also has to be vigilant about checking her emails for spam and other forms of identity theft. She now receives *many* spam emails and texts now and

for the past months, and which she did not typically receive before. Specifically, she has been receiving about 3 or more strange spam emails weekly. These spam emails were not at all similar to ones she had received in the past. She thinks that they are related to HBI's Data Breach since she has only received this type of spam since about the time of the breach or after. The time she spends trying to block these unwanted communications is time that she would rather use in other ways. She cannot figure out any other explanation than that it is related to HBI's Data Breach which included her Private Information.

71. Plaintiff Toussaint is aware that cybercriminals often sell Private Information, and that hers could be abused months or even years after this Data Breach. She is aware that she faces an imminent and substantial risk of identity theft as a result of HBI's Data Breach.

72. Had Plaintiff Toussaint been aware that HBI's computer systems were not secure, she would not have entrusted HBI with her personal data.

PLAINTIFF(S)' AND CLASS MEMBERS' INJURIES

129. To date, Defendant HBI has done absolutely nothing to compensate Plaintiff(s) and Class Members for the damages they sustained in the Data Breach.

130. Defendant HBI has merely offered identity monitoring services for a paltry 24 months through Experian IdentityWorks, a tacit admission that its failure to protect their Private Information has caused Plaintiff(s) and Class great injuries. *See* Exhs. A. This two-year limitation –and its narrow enrollment window of about three months—is inadequate when victims are likely to face many years of identity theft.

92. HBI's offer fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiff(s)' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

93. Furthermore, Defendant HBI's credit monitoring offer and advice (*see* Exh. A) to Plaintiff(s) and Class Members squarely places the burden on Plaintiff(s) and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Defendant merely sent instructions to Plaintiff(s) and Class Members about actions they can affirmatively take to protect themselves.

94. Plaintiff(s) and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

95. Plaintiff(s)' and Class Members' Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

96. Plaintiff(s) and Class Members were damaged in that their Private Information is now in the hands of cyber criminals, sold and potentially for sale for years into the future.

97. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

98. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have been forced to expend time dealing with the effects of the Data Breach.

99. Plaintiff(s) and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

100. Plaintiff(s) and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff(s) and Class Members.

101. Plaintiff(s) and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

102. Plaintiff(s) and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

103. Plaintiff(s) and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

104. Plaintiff(s) and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Finding fraudulent charges;
- b. Canceling and reissuing credit and debit cards;
- c. Purchasing credit monitoring and identity theft prevention;
- d. Addressing their inability to withdraw funds linked to compromised accounts;
- e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- f. Placing “freezes” and “alerts” with credit reporting agencies;
- g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
- h. Contacting financial institutions and closing or modifying financial accounts;
- i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
- j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and
- k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

105. Moreover, Plaintiff(s) and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and

safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

106. Further, as a result of Defendant's conduct, Plaintiff(s) and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

107. Defendant's delay in identifying and reporting the Data Breach caused additional harm. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft.

CLASS ACTION ALLEGATIONS

108. Plaintiff(s) bring this action on behalf of themselves and on behalf of all other persons similarly situated.

109. Plaintiff(s) propose the following Class definition, subject to amendment as appropriate:

All persons whose Private Information was compromised as a result of the May 2022 Data Breach and for which HBI provided notice since May 2022 (the "Class").

110. Excluded from the Class are Defendant's officers and directors, and those of any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from

the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

111. Plaintiff(s) hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

112. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiff(s) at this time. HBI provided notice to state attorneys general that the number is still being investigated and has affected an unknown number of individuals.

113. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff(s)' and Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiff(s) and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant's conduct was per se negligent;
- l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
- m. Whether Defendant was unjustly enriched;
- n. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and
- o. Whether Plaintiff(s) and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

114. Typicality. Plaintiff(s)' claims are typical of those of other Class Members because Plaintiff(s)' Private Information, like that of every other Class member, was compromised in the Data Breach.

115. Adequacy of Representation. Plaintiff(s) will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff(s)' Counsel is

competent and experienced in litigating class actions, including data privacy litigation of this kind.

116. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff(s) and Class Members, in that all the Plaintiff(s)' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

117. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

118. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

119. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

First Count

Negligence

(On Behalf of Plaintiff(s) and Class Members)

120. Plaintiff(s) re-alleges and incorporates the above allegations as if fully set forth herein.

121. Defendant HBI required Plaintiff(s) and Class Members to submit non-public personal information in order to obtain employment and employment benefits as well as other business services.

122. By collecting and storing this data in HBI's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

123. Defendant owed a duty of care to Plaintiff(s) and Class Members to provide data security consistent with industry standards and other requirements discussed herein,

and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

124. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant HBI and its current and former employees and other individuals from whom it collected PII. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

125. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant was bound by industry standards to protect confidential Private Information.

126. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

- f. Failing to timely and fully notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

127. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in businesses who many employees.

128. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

129. Plaintiff(s) and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

130. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff(s) and Class Members, upon information and belief, in an unsafe and unsecure manner.

131. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) to provide adequate, long-term credit monitoring to all Class Members.

Second Count
Negligence *Per Se*
(On Behalf of Plaintiff(s) and All Class Members)

132. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

133. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff(s)' and Class Members' Private Information.

134. Defendant breached its duties to Plaintiff(s) and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff(s)' and Class Members' Private Information.

135. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

136. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff(s) and Class Members, Plaintiff(s) and Class Members would not have been injured.

137. The injury and harm suffered by Plaintiff(s) and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it failed to meet its duties, and that Defendant's breach would cause Plaintiff(s) and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

138. As a direct and proximate result of Defendant's negligent conduct, Plaintiff(s) and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Third Count
Breach of Implied Contract
(On Behalf of Plaintiff(s) and Class Members)

139. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

140. When Plaintiff(s) and Class Members provided their Private Information to Defendant HBI in exchange for Defendant HBI's employment, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

141. Defendant HBI solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff(s) and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

142. In entering into such implied contracts, Plaintiff(s) and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

143. Plaintiff(s) and Class Members provided their Private Information and their labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

144. Plaintiff(s) and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

145. Plaintiff(s) and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

146. Plaintiff(s) and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

147. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

148. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

149. Plaintiff(s) and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

150. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

Fourth Count
Invasion of Privacy
(On Behalf of Plaintiff(s) and All Class Members)

151. Plaintiff(s) re-allege the above allegations as if fully set forth herein.

152. Plaintiff(s) and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

153. Defendant's conduct as alleged above intruded upon Plaintiff(s)' and Class Members' seclusion under common law.

154. By intentionally failing to keep Plaintiff(s)' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff(s)' and Class Members' privacy by:

- a. Intentionally and substantially intruding into Plaintiff(s)' and Class Members' private affairs in a manner that identifies Plaintiff(s) and Class Members and that would be highly offensive and objectionable to an ordinary person; and
- b. Intentionally publicizing private facts about Plaintiff(s) and Class Members, which is highly offensive and objectionable to an ordinary person; and
- c. Intentionally causing anguish or suffering to Plaintiff(s) and Class Members.

155. Defendant knew that an ordinary person in Plaintiff(s)' or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

156. Defendant invaded Plaintiff(s)' and Class Members' right to privacy and intruded into Plaintiff(s)' and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

157. Defendant intentionally concealed from and delayed reporting to Plaintiff(s) and Class Members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

158. The conduct described above was at or directed at Plaintiff(s) and the Class Members.

159. As a proximate result of such intentional misuse and disclosures, Plaintiff(s)' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff(s)' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

160. In failing to protect Plaintiff(s)' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff(s)' and Class Members' rights to have such information kept confidential and private. Plaintiff(s), therefore, seek an award of damages on behalf of themselves and the Class.

Fifth Count
Unjust Enrichment
(On Behalf of Plaintiff(s) and Class Members)

161. Plaintiff(s) re-allege the above allegations as if fully set forth herein. Plaintiff(s) bring this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of contract count above.

162. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments for security of Private Information that was spent (or not spent) on behalf of Plaintiff(s) and the Class Members.

163. As such, a portion of the fruits of the labor of Plaintiff(s) and the Class Members is to be used to provide a reasonable level of data security, and the amount of money previously expended on computer and data security is known to Defendant, as is the amount that would have been required to maintain sufficient data security, had Defendant done so prior to this Data Breach.

164. Plaintiff(s) and Class Members conferred a monetary benefit on Defendant. Specifically, they provided labor and services to Defendant and/or its agents and in so doing were required to provide Defendant with their Private Information. In exchange, Plaintiff(s) and Class Members should have received from Defendant wages and benefits that were the subject of the transaction as well as a promise to protect their Private Information with adequate data security.

165. Defendant knew that Plaintiff(s) and Class Members conferred a benefit which Defendant accepted. Defendant profited from Class Members' labor and used the Private Information of Plaintiff(s) and Class Members for business purposes.

166. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff(s) and Class Members by utilizing cheaper, ineffective security

measures. Plaintiff(s) and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

167. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff(s) and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

168. Defendant failed to secure Plaintiff(s)' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff(s) and Class Members provided.

169. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

170. If Plaintiff(s) and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

171. Plaintiff(s) and Class Members have no adequate remedy at law.

172. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with

efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff(s) and Class Members.

173. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

174. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff(s) and Class Members, proceeds that they unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff(s) pray for judgment as follows:

- a) For an Order certifying this action as a class action and appointing Plaintiff(s) and their counsel to represent the Class;
- b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of

Plaintiff(s)' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff(s) and Class Members;

- c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;
- d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- e) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff(s) and the Class;
- f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- g) For an award of punitive damages, as allowable by law;
- h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- i) Pre- and post-judgment interest on any amounts awarded; and
- j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff(s) demand a trial by jury on all claims so triable.

Dated: October 13, 2022

Respectfully submitted,

/s/ Joel R. Rhine

Joel R. Rhine

Martin A. Ramey

RHINE LAW FIRM, P.C.

1612 Military Cutoff Road, Suite 300,
Wilmington, NC 28403

Telephone: (910) 772-9960

Facsimile: (910) 772-9062

Phone: (910) 772-9960

jrr@rhinelawfirm.com

mjr@rhinelawfirm.com

Gary E. Mason*

Danielle Perry*

Lisa A. White*

MASON LLP

5301 Wisconsin Avenue, NW
Suite 305

Washington, DC 20016

Tel: (202) 429-2290

gmason@masonllp.com

dperry@masonllp.com

lwhite@masonllp.com

Attorneys for Plaintiff

**pro hac vice to be filed*